

ONLINE SAFETY AWARENESS

JUNE 2018



INTRODUCTION

During the Dispute Resolution Commission's last mediator certification renewal period, some mediators received fraudulent emails. The emails were sent by individuals or groups seeking to obtain mediator credit card or other financial information. The Commission wants to keep your information private and secure.

This presentation will provide users with the information and tools needed to safely communicate using email.

We will be looking at two tactics that malicious individuals use to obtain your personal information:
Phishing and Pharming.



WHAT IS PHISHING?

- Sending fake emails to fool users into taking an action, such as clicking on a link or opening an attachment, in order to complete a malicious action.
- Why do malicious users phish?
 - Steal usernames and passwords
 - Receive payment under false pretenses
 - Access other business/personal information without permission
 - Infect an organization's technology assets or an individual user's computer with malware



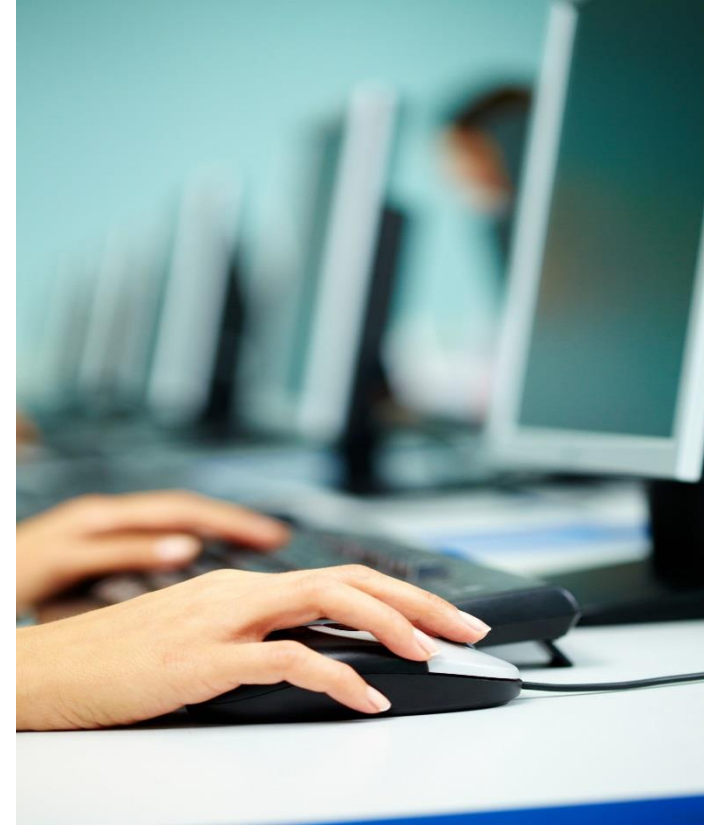
WHAT IS PHARMING?

- A common approach is a fake email or website made to look like a known, legitimate site to get users to attempt to log in. Once users do this their username and password are stored by hacker(s).
- Why pharm?
 - Sell usernames and passwords for identity theft of others
 - Make fraudulent purchases
 - Gain unauthorized access to email, banking, and other services



IDENTIFYING PHISHING EMAILS

- There are ways to identify phishing emails. These include:
 - Checking the email address of the sender
 - Paying attention to the website addresses of any links
 - Looking for poor grammar and misspellings
- The next three slides will provide specific examples of fraudulent emails.



SAMPLE 1

“All the best”
is not a
greeting for
an email.

The link
provided has a
.nl domain
instead of .com
or .org. This is a
foreign website
(most likely for
the
Netherlands).

From: DRC Mediators <julsikor@pg.gda.pl>
Date: November 17, 2017 at 6:19:08 AM EST
To: <wmcelwee@mcclweefirm.com>
Subject: Invoice 0241530914 reminder

All the best ,

Invoice Notification. Date:17 Nov 17. Got questions? Just give me a call at 01383 867029.

Invoice 0241530914 reminder:
<https://juuve.nl/beatrixkwartier/wp-content/LLC/>

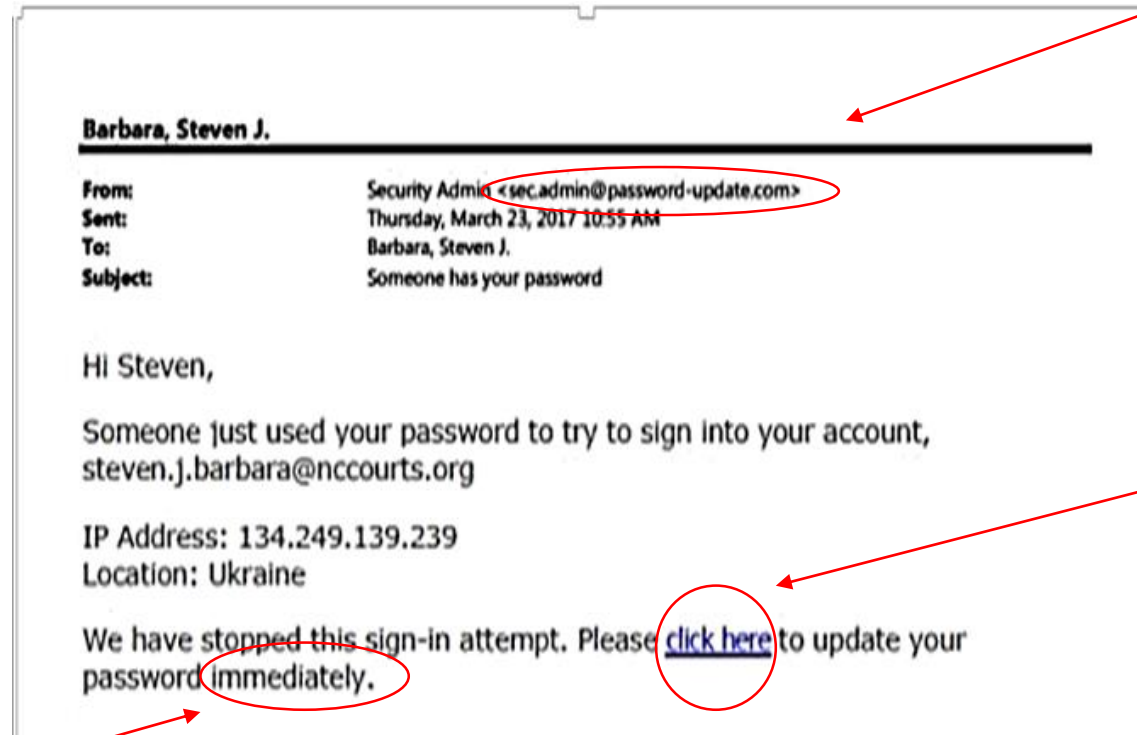
Sincerely,
DRC Mediators

The sender's email
address is non-
Judicial **AND** non-
US (.pl domain is
for Poland)

The phone
number
provided is not
a US number



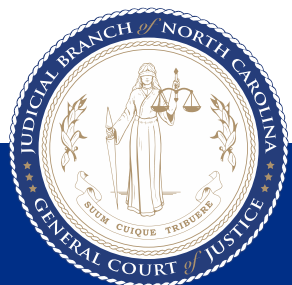
SAMPLE 2



The sender is a non-Judicial Branch email address

On the original email, if you hover over this link, it will show it is an external website

Creates a sense of urgency to take action



SAMPLE 3

This is an external website. Do not click on suspicious links

Robinson, Maureen M.

From: [REDACTED]
Sent: Friday, November 17, 2017 10:59 AM
To: DRC Mediators
Subject: You might want to let mediators know that your email has been hacked...

See below. Thought you would want to know that your email has been hacked.

Thanks,
[REDACTED]

-----Original Message-----

From: DRC Mediators [mailto:reservas@hotelpalaceguayaquil.com.ec]
Sent: Thursday, November 16, 2017 7:48 PM
To: [REDACTED]
Subject: #841234/XL#QFL/2017 (17 Nov 17) Invoice Notice

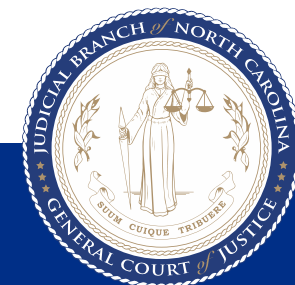
Greetings,

I called you, but could not reach you the other day, please reply back about this past due invoice asap.

<http://www.only-simba.com/Download/tomeverlync@gmail.com>

Good Day,
DRC Mediators

This is not an official email address



WHAT TO DO AFTER THE ATTACK



- If you become a victim of a phishing attack, follow these steps:
 - Immediately change affected account passwords
 - Watch for unauthorized charges to your financial accounts
 - Report any suspicious emails to abuse@nccourts.org and notify the NCDRC's office

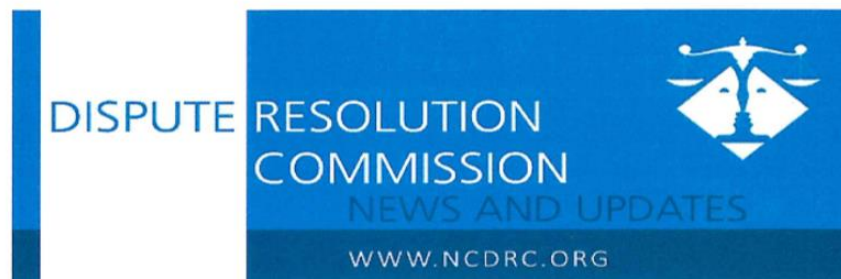


REVIEW

- The NCDRC will never ask you to:
 - Confirm your renewal
 - Verify your credit card
 - Provide bank account information
- All official emails will come from DRCMediators@nccourts.org
- All emails from the NCDRC will resemble the email to the right.

Robinson, Maureen M.

From: DRC Mediators
Sent: Friday, June 30, 2017 9:07 AM
To: DRC Mediators
Subject: Mediator Certification Renewal Notice - Starts July 1, 2017



June 30, 2017

919-890-1415

To: All Certified MSC, FFS and Clerk Mediators
From: Leslie Ratliff, Executive Director
Re: Mediator Certification Renewal FY 2017-2018

It is time to renew your mediator certification(s) for FY 2017-2018. The Commission thanks you for your efforts on behalf of our courts and citizens during FY 2016-2017, and hopes that you will continue to serve North Carolina's courts and citizens as a mediator in the coming year.

The renewal period for both active and inactive mediators is from **July 1, 2017**, through **September 30, 2017**. The Commission works hard to hold the line on expenses and the renewal amount remains unchanged since 2001 – \$140.00 for a single and \$200.00 for a dual certification. There is no additional charge for certification in the Clerk Mediation Program.

Your online certification renewal application must be submitted and payment received by September 30, 2017. If payment is made by check, the check must be postmarked on or before September 30, 2017. If your application and payment are not received on or before September 30, 2017, you will be assessed a \$30 late fee.



ADDITIONAL RESOURCES

- Review [this document](#) with more tips on identifying phishing emails
- Visit staysafeonline.org
- Consider subscribing to this newsletter for ongoing security awareness:
[Ouch Newsletter](#)



PRINTABLE CHECKLIST

- ❑ Check the address of the sender. Verify it is someone you know.
- ❑ Look for:
 - ❑ Poor grammar
 - ❑ Misspellings
 - ❑ Unprofessional tone
- ❑ Be wary of clicking links
- ❑ Report and delete any suspicious emails





THANK YOU

Steven Barbara

Steven.J.Barbara@nccourts.org

